Realizing the Army Net-Centric Data Strategy (ANCDS) in a Service Oriented Architecture (SOA)

Michelle Dirner
Army Net-Centric Data Strategy (ANCDS) Center of Excellence (CoE)
michelle.dirner@us.army.mil

Eric Yuan
Booz Allen Hamilton
yuan_eric@bah.com

James Blalock
Army CIO / G6 Architecture, Operations & Space Directorate
james.blalock@us.army.mil

Abstract

Net-Centric Operational Warfare (NCOW) describes how the United States Department of Defense (DoD) will conduct business operations, warfare, and enterprise management in the future. It is based on the information technology (IT) concept of an assured, dynamic, and shared information environment that provides access to trusted information for all users, based on need, independent of time and place. NCOW is an information-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters. This enables shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization. In essence, network-centric warfare translates information superiority into combat power by effectively linking knowledgeable entities in the battlespace.

The DoD has mandated that the Global Information Grid (GIG) will be the primary infrastructure capability to support NCOW. Under this directive, all advanced weapons platforms, sensor systems, and command and control centers are eventually to be linked via the GIG. In the DoD vision, implementation of this massive integration effort relies on a Service Oriented Architecture (SOA) model and Net-Centric Data Strategy approach, along with extensive use of the Extensive Markup Language (XML) and other web service standards.

This paper attempts to explain in plain language the inter-relationship between the various IT components that will provide the Net-Centric environment and assist the Army in migrating towards the Net-Centric Warfare concept.

1. Army Net-Centric Data Strategy (ANCDS) Overview

To support warfighters in today's rapidly-changing threat environment, the Department of Defense (DoD) is transforming itself towards Net-Centricity. The heart of the net-centric approach is information sharing: The ability to access information, use it, and collaborate it with others is the key to an agile DoD enterprise. The vision for information sharing in the DoD, as stated in the recently published DoD Information Sharing Strategy [1], is:

> *Deliver the power of information to ensure mission success through an agile enterprise with freedom of maneuverability across the information environment.*

Amid all the net-centric activities and initiatives lays a key enabler to this vision: the Net-Centric Data Strategy (NCDS). As DoD CIO John Grimes puts it, "It is all about the data. To successfully implement a secure enterprise-level net-centric operations capability for the warfighter, we must move away from highly tailored programs that manipulate data and move to exposing the data in a timely fashion."[2] The DoD Directive 8320.02, Data Sharing in a Net-Centric Department of Defense [3], established seven (7) goals to make data:

1) *Visible* – Who has what data available?
2) *Accessible* – Where is this data and in what format?
3) *Understandable* – What does this data mean?

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
20 MAY 2008	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Realizing the Army Net-Centric Data Strategy (ANCDS) in a Service Oriented Architecture (SOA)	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Army Net-Centric Data Strategy (ANCDS) Center of Excellence (CoE)**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
AFCEA-GMU C4I Center Symposium "Critical Issues In C4I" 20-21 May 2008, George Mason University, Fairfax, Virginia Campus, The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**18**	

4) *Trusted* – Is this data trustworthy, accurate, and authoritative?
5) *Interoperable* – Can my application use the data?
6) *Responsive* to users needs – Is the data applicable and timely?
7) *Institutionalized* – What and who governs the definition, lifecycle, and use of this data?

The data goals are organizationally facilitated by the formation of Communities of Interests (COI), which are collaborative groups of users who must exchange information in pursuit of their shared goals, missions, or business processes.

The Army, like other DoD Components, has been focusing primarily on the first three (3) data goals, and has made significant progress towards net-centric data sharing from organizational, process, and technological fronts. Specifically,

- Through the organizational construct of Mission Areas (MA) and Domains, the Army actively manages and participates in the COI activities. The Army Net-Centric Data Strategy Guidance document [4] provides general guidance to assist the Army Mission Areas, Domains, and COIs in understanding their roles and responsibilities as they affect the Army's data strategy.
- The Army has stood up the Army Data Harmonization and Integration Working Group (ADHIWG) to assist in data governance, share lessons learned, and represent Army enterprise positions.
- The Army NCDS Center of Excellence (CoE) is also established to provide subject matter expertise to COIs to assist in Information Exchange Standards and Specifications (IESS), Data Engineering, Data Governance (e.g. Certification, Validation and administration), and Configuration Management (CM).
- The Army recognizes the importance of Service Oriented Architecture (SOA) technologies as enablers to NCDS goals. It has established a SOA Center of Excellence and is actively developing its SOA Foundation capabilities through leveraging DoD Net-Centric Enterprise Services (NCES).

Implementing the NCDS for the Army enterprise, however, is not without its challenges, some of which are identified in the Program Decision Memorandum (PDM) III findings [5]. In particular, issues such as COI governance, management structure, and integration with the current acquisition processes (e.g., Joint Capabilities Integration Development System (JCIDS) and IT Portfolio Management) are still being addressed. Even putting the organizational and policy issues aside, it is often easy to overlook the daunting technical challenges of realizing the value of information sharing in the Army's unique operational environment. Just to name a few:

- How would the Army Data Strategy transform the existing / legacy systems while seamlessly maintaining their capabilities to support the soldiers at war?
- How would the data strategy bridge the information gap to the warfighters on the tactical edge while at the same time interoperate with the DoD and Joint enterprises? More specifically, the data strategy needs to support mobile forces with decentralized and disadvantaged networks.
- How would the Army architect the data sharing capabilities to support the doctrinal goals such as Force Modularity, Train as You Fight, Full-spectrum Operations, and Reachback?

The Army is looking to SOA as the technology and infrastructure enabler to help overcome these challenges. This paper is intended to describe the "end state" paradigm of the Army's data sharing environment and illustrate how SOA strategies, tenets and technologies can be applied to realize that vision.

2. Conceptual Architecture for Net-Centric Data Sharing

In a fully operational Net-Centric enterprise, the seven data goals become reality so that the right data can get to the right people at the right time, in a secure fashion. A conceptual view for such an enterprise is depicted in **Error! Reference source not found.**. The picture reflects the following paradigm shifts in the data sharing philosophy:

- *From ownership to stewardship*. Data producers no longer holds tightly to the data and only uses it for predetermined needs, but instead exposes and publishes data to the enterprise to benefit also the unanticipated users.
- *From need-to-know to right-to-know*. Data consumers, once authorized, can access the enterprise to obtain information that is critical to doing his or her job.
- *From systems to services*. The traditional thinking of building data gathering and processing capabilities as hardware boxes and packaged

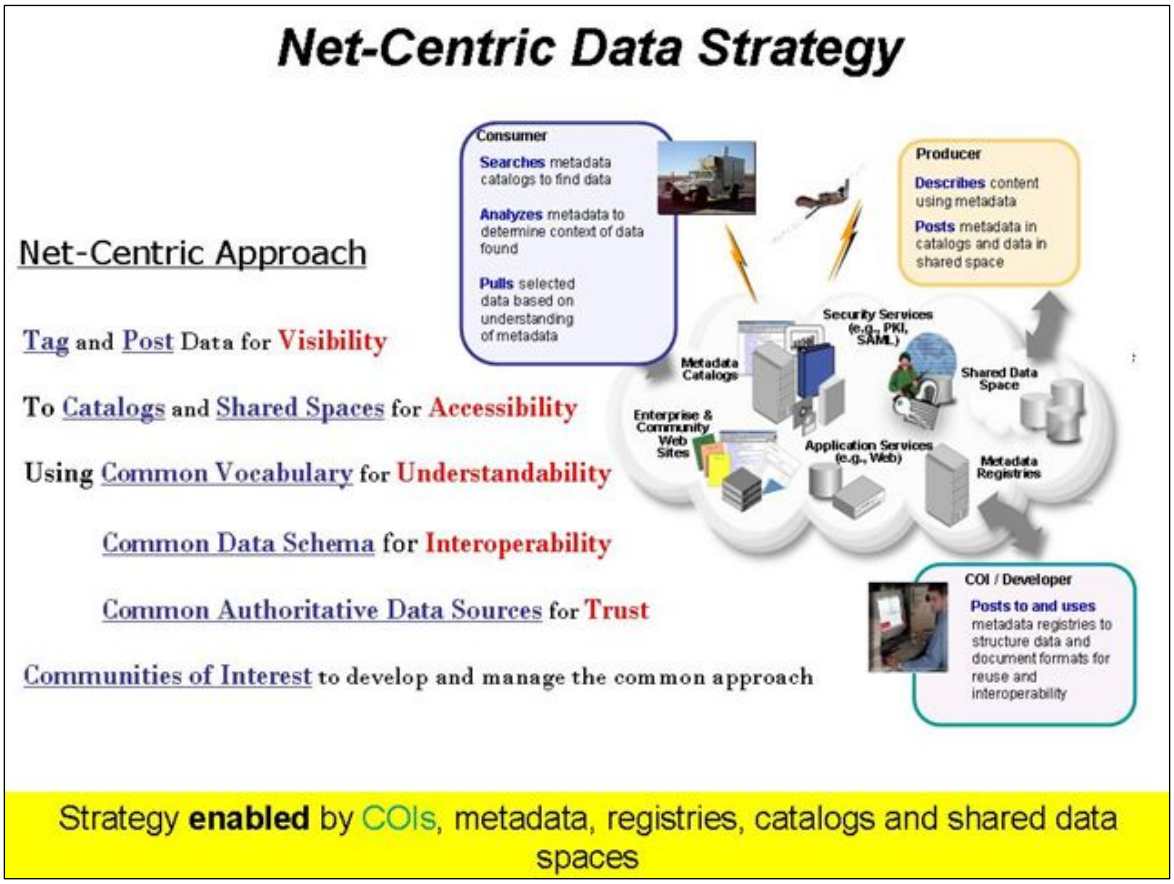


Figure 1: Net-Centric Data Sharing Concepts

applications will give way to loosely coupled, reusable, and standards-based services.

- *From stovepipes to enterprise*. Data sharing infrastructure are put in place so that data is no longer hidden in silos and behind proprietary interfaces, but is accessed and delivered freely across the Enterprise Information Environment (EIE) supported by enterprise-wide "plumbing".
- *From programs to portfolios*. From the governance perspective, the buildup of data-centric capabilities is not just the responsibility of individual acquisition programs but requires increased oversight from the Army enterprise-wide IT Service Portfolio Management (SPM).

From the technology perspective, the conceptual architecture reflects the major mechanisms / best practices for making data visible, accessible, understandable, and trusted:

- Tagging data with *metadata* for visibility;
- *Registries* and catalogs that facilitate federated search across the enterprise;
- The use of data schemas, vocabularies, and other *Information Exchange Standards and Specifications (IESS)* for data understandability and interoperability;
- The designation of *Authoritative Data Sources (ADS)* to provide trusted data
- The need for enterprise infrastructure such as security, discovery, and management

Many of these recommendations are described in detail in both DoD and Army NCDS guidance documents ([4], [6]). It is important to note that, even though the Net-Centric data vision is the same across the Army and DoD, the instantiation of the capabilities do not necessarily follow a one-size-fits-all approach. Different COIs, domains, or mission areas may choose to define their own architectures and implementations based on specific operational needs, while still adhering to the above NCDS concepts and guidance.

3. SOA: Enabler to Net-Centric Data Sharing

So how can the Army realize its NCDS vision and move from today's platform- and system-centric data world to the aforementioned end-state paradigm? One essential piece of the puzzle is the utilization of the Service Oriented Architecture. SOA is recognized across the DoD as a key to Net-Centric transformation, and as such plays a vital role in supporting the ANCDS. There are four (4) aspects of SOA that may be leveraged to meet the Army's data needs: SOA tenets and principles, Core SOA standards, SOA enterprise infrastructure, and SOA-enabled data sharing technologies.

3.1 SOA Tenets and Principles

The "A" in SOA stands for Architecture, therefore SOA is first and foremost a set of architecture principles and design tenets. In other words, SOA prescribes certain ways in which systems and capabilities should be built and how they should interact with one another. In the context of realizing the Net-Centric Data Strategy, the key principles and tenets of SOA that are most applicable include:

- *Loose coupling through well-defined interface specifications*—SOA eliminates the so-called "N^2" problem of point-to-point system integration by defining non-proprietary interface specifications. Loose-coupling ensures that the degree of dependency between services and their consumers be kept to a minimum, and that interactions are executed through well-defined interfaces "contracts", thereby reducing the dependencies on internal implementation-specific details. This concept is illustrated in Figure 2.

Army Data Strategy Implications

The interface specification- driven approach is the key to data accessibility. More importantly, the principle of loose-coupling can be applied to the N^2 problem of point-to-point data integration by defining community-embraced common data specifications for information exchange, and by adopting core data specifications already defined by the Army, DoD, or the federal government.

- *Interoperability through the reliance on open standards*—the architecture should be based on open standards for improved interoperability and reduced reliance on proprietary platforms, programming languages, and products.

Army Data Strategy Implications

*There are a vast number of IT open standards; from the data perspective, however, the focus should be on the **information exchange** standards rather than implementation standards such as J2EE. The information exchange standards for consideration within the Army may come from the commercial industry, but may also come from the larger Federal Government and DoD community.*

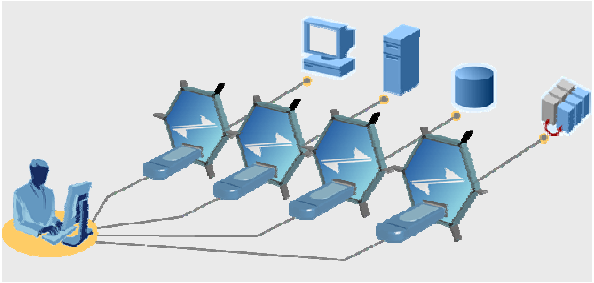


Figure 2: Exposing Info Assets as Services

- *Agility through composability*—services can be composed of other services and should be designed so that they can be composed into other services or applications. This reduces the time and effort to create new services and applications or adapt to changes—thus leading to increased agility.

Army Data Strategy Implications

As the Army architects its data-sharing capabilities and supporting infrastructure, agility will be a key requirement. New threats and changing missions will require changes in existing doctrines and TTPs, which will in turn require changes in the supporting data capabilities. The latter must be designed to be agile in order to be able to adapt quickly to such changes.

- *Leveragability through reuse of legacy systems*—contrary to the "rip and replace" approach, legacy systems should be wrapped with services to expose and share the valuable functionality and data contained within them.

3.2 Core SOA Standards

Under a SOA, a set of network-accessible operations and associated resources are abstracted as a "service". The service is described in a standard fashion, published to a service registry, discovered by a service consumer, and invoked by a service consumer – this is often referred to as the "Publish-Discover-Interact triad" pattern.

Although the principles of SOA have been around for many years, it is the contemporary implementation technologies such as the eXtensible Markup Language (XML) and Web Services that has fueled the widespread popularity and adoption of SOA. XML is a text-based data format that allows the "tagging" of data and metadata using well-defined syntax rules. Three XML-based standards form the foundation of the SOA Web Services "protocol stack": SOAP, Web Service Description Language (WSDL), and Universal Discovery, Description, and Integration (UDDI).

These widely-adopted standards help ensure the visibility and accessibility of data assets. Even though these standards have so far been used in the strategic and operational enterprise environments, technologies and solutions are emerging to apply them to the tactical environments as well.

3.3 Enterprise SOA Infrastructure

The creation of services alone does not constitute an SOA. A set of SOA infrastructure capabilities is needed to provide a robust foundation to facilitate the interaction between service providers and consumers. As the Army plans for the creation of its net-centric data sharing environment, the minimum set of capabilities supported by the underlying infrastructure should include the following:

- *Service Discovery*—provides the capabilities to publish and discover data, metadata, and services. Technologies that provide such capabilities include directory servers, metadata registries, service registries and repositories.
- *Security*—provides information assurance capabilities such as controlling access to services and data, management of user profiles and access control policies, message-level encryption and non-repudiation, etc.
- *Reliable Messaging*—provides the capability to reliably exchange messages between services and their consumers. Examples of technologies that provide this capability include message-oriented-middleware (MOM) and enterprise service buses (ESB).
- *Message and Protocol Mediation*—provides the capability to adapt data formats and exchange protocols to enable interoperability in a heterogeneous environment. Most ESBs provide data and protocol adaptation capabilities.
- *Service Orchestration*—provides the capability to compose and orchestrate individual services into larger aggregates of functionality or business processes. Example technologies include Business Process Execution Language (BPEL) and Business Process Management (BPM) orchestration engines.
- *Enterprise Service Management*—provides the capabilities to monitor and control services to ensure compliance with defined contracts and service level agreements.

The Army is in the process of establishing a set of SOA Foundation (SOAF) capabilities that are distributed across the enterprise, providing interoperability with the larger DoD and GIG enterprise but also helping extend SOA support to the warfighters on the tactical edge.

3.4 SOA Enabled Data Sharing Technologies

True data-sharing can only be achieved when consumers of the data are able to interoperate with the providers and understand the data. While the core SOA technologies enable data visibility and accessibility, the data-sharing technologies are what enable interoperability and understandability. Interoperability and understandability, though related, are two distinct characteristics that require different approaches and technologies to achieve:

Interoperability is achieved when consumers can comprehend and process the syntax and structure of the data. Today the most widely used technology to enable this is XML. In accordance with the ANCDS and its corresponding implementation guidance, COIs should create standard representation formats to allow the interoperable exchange of the data that they steward. Such formats should be defined using XML Schema so that they can be referenced within the descriptions (i.e. WSDLs) of the services that will be created to allow access to that data.

Understandability builds on top of interoperability to allow consumers to comprehend the actual meaning of the data once they are able to process its syntax and structure. Enabling machines to truly understand the meaning of the data they are processing has been one of the holy grails of computing for many years.

Recently, advances in Semantic Web technologies have been showing some promise in this area. The creation of formal ontologies using standards such as Resource Description Framework (RDF) and Web Ontology Language (OWL) can allow COI-created vocabularies to be expressed in machine-processable formats so that data understandability can be automated. Such semantic representations will enable more intelligent data searches and even machine reasoning and inferencing atop the traditional data processing functions.

4. Combining Data and SOA Strategies to Guide Net-Centric Data Migration

After learning about the SOA capabilities and technologies, a decision maker would naturally ask the question, "That all sounds great, but how does it help me execute the data strategy?" To answer this question, it may help to take a closer look at the relationship between NCDS and SOA, and the different roles they play in Net-Centric information sharing. A simple SOA-enabled data exchange example can be used to illustrate this:

- An information asset such as an ADS would like to exchange data within the enterprise. First, the information asset offers up the contents to be exchanged in the form of XML documents. The XML document represents a set of data that is usually transmitted for a specific business purpose.
- The XML document is formatted according to a "template", which is usually in the form of XML schemas along with other business rules such as standard metadata tags or common data elements for a particular COI / domain.
- The XML document constitutes the *payload* that is enclosed in a "message", which provides routing information, security controls, and other information needed to deliver the content. Technically speaking, the message wrapper is also defined using standard formats such as WSDLs, which "imports" the XML schemas to describe the payload.
- The message is then transmitted using the appropriate network protocols and transport mechanisms.

This example, shown in Figure 3, shows the different focus of SOA and data strategies:

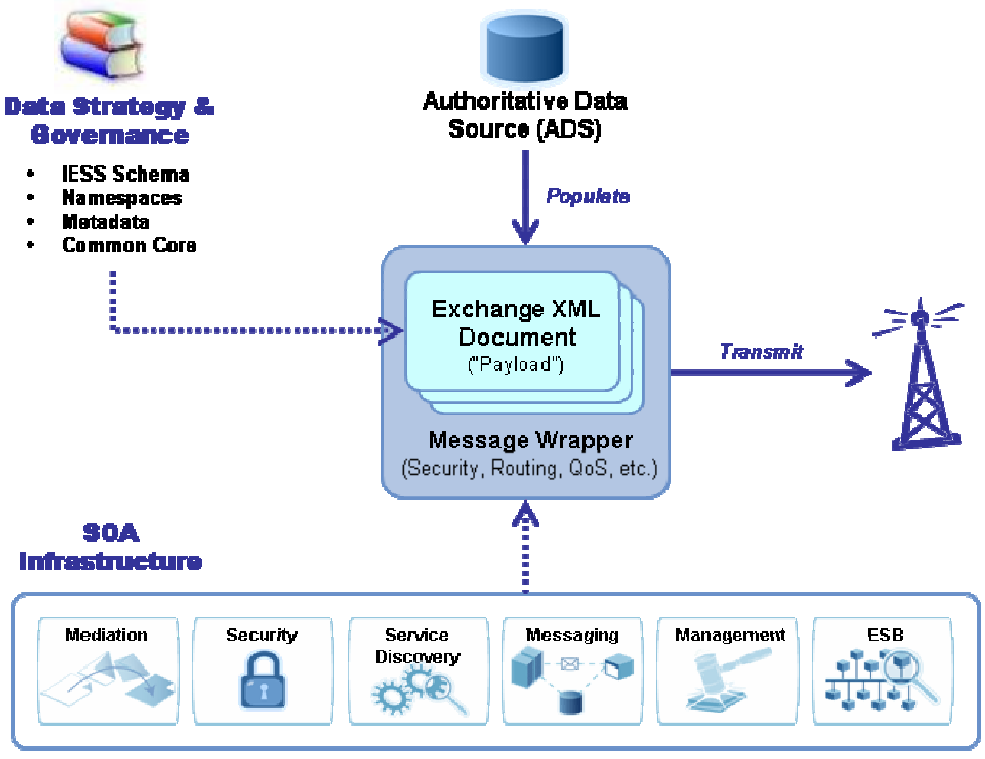


Figure 3: Data Strategy and SOA Roles in Data Exchange

The data strategy focuses on formulating the content or *payload* of the data exchange. It dictates the schemas, semantics, and layouts of the data, and provides both policy and technical guidance to make sure the data being exchanged is interoperable and understandable. The SOA strategy, on the other hand, focuses on the *messaging* aspect of the data exchange. It defines the message wrapper around the payload and, more importantly, provides enterprise-strength "plumbing" that ensures the message can be exchanged between a provider and a consumer in a loosely-coupled, secure, timely, and managed fashion.

More formally,

- Enterprise data strategies in general focus on issues such as data governance—identifying data assets that need to be managed and shared at an enterprise level; identifying or establishing authoritative sources of that data; and defining the roles and responsibilities of data producers and data consumers to ensure proper management and usage of that data. Governance structures (e.g. mission areas and COIs) are established to manage the creation of logical data representations (at both structural and semantic levels) to enable interoperability and ensure a common understanding across the enterprise. At a high level, these are many of the aspects that are covered by the directives in the ANCDS.
- SOA strategies on the other hand focus on the creation of an environment in which functionality and data can be exposed as modular units of software services to be shared across the enterprise. The strategy provides a framework for managing those services and mechanisms to discover and use the services and associated data. It provides the capabilities to orchestrate and compose individual services into larger units of functionality to match specific application needs. All of this is supported in heterogeneous environments through technologies that can mediate differences in data formats and application protocols.

Looking from another perspective, however, the different focuses of a data strategy versus an SOA strategy make them in fact **complementary** – The data strategy by itself does not address completely, the details for a common framework and mechanisms for sharing data across heterogeneous environments in a seamless manner. This is precisely the purpose of the services environment that is created through an SOA strategy. On the other hand, the SOA strategy just provides a generic framework for exposing and sharing services—it says nothing about what should be shared through those services. This is where the data strategy comes in—it prescribes a strategy for identifying the data to be shared, where that data should be coming from (i.e. authoritative sources) and standard representations for sharing that data.

A pictorial view of the SOA – Data relationships and overlaps is given in Figure 4.

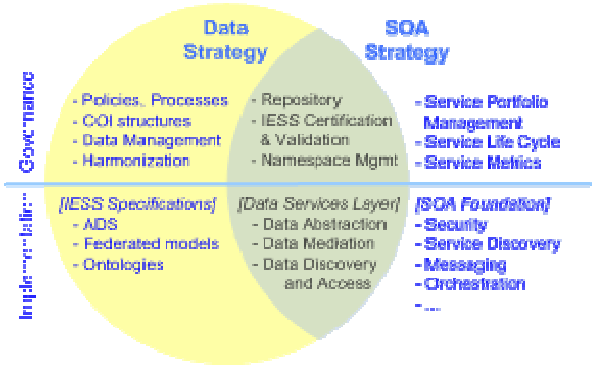


Figure 4: Relationship between Data and SOA Strategies

It is worth noting that, during technology implementation, the intersection of these two strategies results in the creation of an enterprise *data services layer* that enables sharing and management of data that is distributed across the enterprise. The data services layer will be described in detail in the next section.

The close alignment of the Army Data and SOA strategies and the synergy between the two will help expedite the migration process towards building truly Net-Centric data capabilities, improve the effectiveness of enterprise governance, and increase community participation. The transformation process is illustrated in Figure 5.

5. The Army Data Services Layer (ADSL): Net-Centric Data Strategy in Action

As an intersection between data strategy and SOA, the data services layer serves as an abstraction of data-centric capabilities instantiated in a SOA environment. A high-level "portfolio view" of the ADSL is depicted in Figure 6. Without going into a lot of technical details, the ADSL represents the following families of data services:

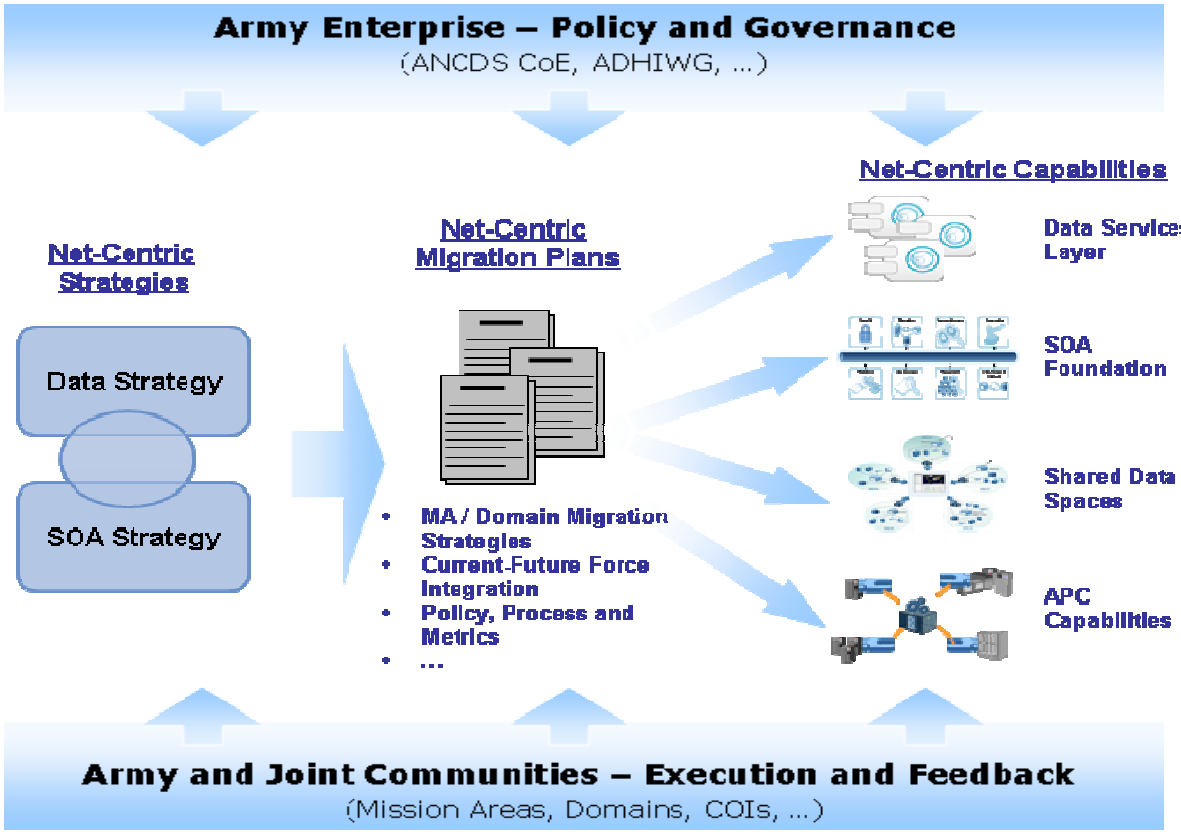


Figure 5: Data and SOA Strategies Driving Net-Centric Transformation

- *Data Management*, providing the persistence and stewardship of data "at-rest";
- *Data Governance* which captures and governs the metadata in a repository, at both structural and semantic levels. Such metadata is made available across the enterprise, allowing for "deep" data visibility;
- *Data Abstraction*, which establishes common standards and authoritative data sources allowing for data discoverability;
- *Data Access*, exposing interfaces to search, retrieve, and manipulate data;
- *Data Mediation*, intended to bridge the gap among different data formats, vocabularies, and semantics, making data understandable and usable to the consumers who are otherwise unable to make use of the data;
- *Data Utilization*, consisting of the set of end-to-end composable applications that are built upon the other "atomic" data services; these applications are user-oriented and directly enable warfighters and decision makers to use data within and outside of the Army to satisfy mission needs.

The ADSL is not a single physical capability. Rather, it may be viewed as a virtual data tier for the Army enterprise, accessible and available on the LandWarNet. Some services, such as Data Mediation, may be hosted at the APCs, while others may reside in a particular theater, a program of record, or even a lab. Nonetheless, collectively define all data services families herein offers many benefits. First, it allows the enterprise to have a "big picture" view of the combined capabilities. It also gives way to easier governance and oversight from a Service Portfolio Management (SPM) perspective. Furthermore, the ADSL portfolio view can be used as a tool to define the "Capability over Time" roadmap, allowing for incremental build-up of chunks of data sharing functionality. In a truly Net-Centric enterprise, the "Net" eventually becomes *the* application and *the* data asset; the data services layer is simply a first step towards this vision.

To develop the ADSL, just like any other enterprise SOA capabilities, the following steps need to be taken:

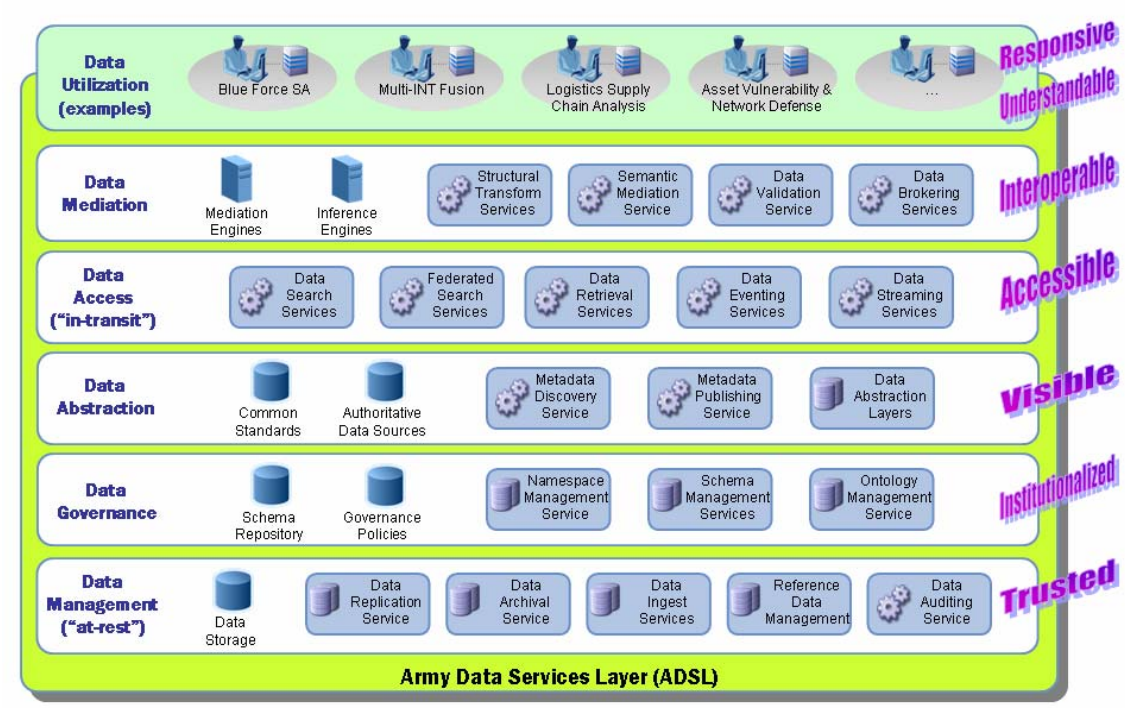


Figure 6: Data Service Layer Defined

- Develop the *Reference Architecture* that prescribes the data service use cases, interaction dynamics, behavior models, and interoperability profiles;
- Develop the set of *Service Interface Specifications* for each individual services or service families, including implementation guidance;
- Develop a *Reference Implementation* that can serve as a concrete, functioning example of the Reference Architecture, to reduce risks and prove out the approach;
- Acquire and deploy the portfolio of ADSL capabilities from vendors and integrators, which are governed and certified by the Reference Architecture and Service Specifications.

Implementing the ADSL involves more than just technology. The recently published DoD Information Sharing Strategy [1] establishes five touchstones: Culture, Policy, Governance, Economics and Resources, and Technology and Infrastructure. The Army is aggressively examining operational scenarios and systems architecture in applying modular force structure, TPPU and SOA concepts to address the operational, acquisition and organizational aspects of Army Net-Centric data transformation.

6. Summary

NCOW concepts of increased combat power by linking knowledgeable entities in the battlespace can only be achieved through the combined and complementary, SOA and Data strategies. The alignment and integration of these IT strategies in implementation efforts lead to the net-centric environment that enables enhanced situation awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a greater degree of self-synchronization – all through leveraging the warfighters' most important strategic asset: *their data*.

7. References

[1] DoD. The DoD Information Sharing Strategy. Washington: DoD, May 2007.

[2] The Honorable John J. Grimes. Enabling Technologies for Net-Centricity – Information on Demand, CrossTalk July 2007 issue. Washington: DoD, July 2007. < http://www.stsc.hill.af.mil/CrossTalk/2007/07/index.html>

[3] DoD. DoD Directive 8320.02, Data Sharing in a Net-Centric Depart of Defense. Washington: DoD, December 2004.

[4] Army. Army Net-Centric Data Strategy Guidance, Version 1.5. Arlington, VA: Army CIO/G6, May 2007

[5] DoD. Implementing the Net-Centric Data Strategy Process and Compliance Report. Washington: DoD CIO, August 2006.

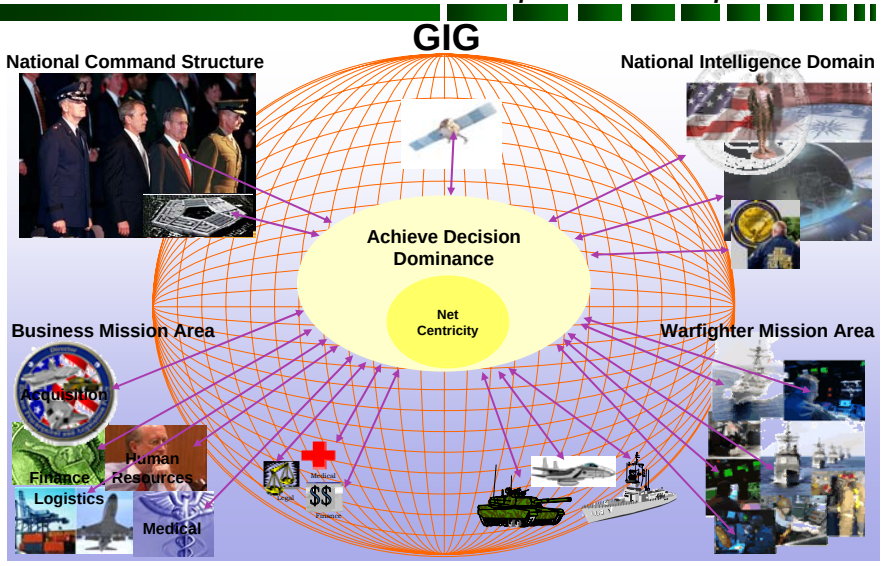
[6] DoD. DoD 8320.02-G Guidance for Implementing Net-Centric Data Sharing. Washington: ASD/NII, April 12, 2006

Realizing the Army Net-Centric Data Strategy (ANCDS) in a Service Oriented Architecture (SOA)

A presentation to GMU/AFCEA symposium "Critical Issues in C4I"

Michelle Dirner, James Blalock , Eric Yuan

Net-Centricity Vision
Operational Concept Notional OV-1

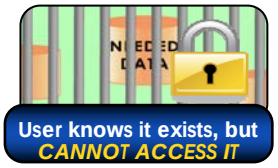


Deliver the power of information to ensure mission success through an agile enterprise with freedom of maneuverability across the information environment.

2

Current Information-Sharing Challenges

Visible?



Accessible?

Understandable?

3

Source: OASD(NII)I/DoD CIO COI Training Package

Net-Centric Data Sharing Concepts

Net-Centric Approach

Tag and Post Data for Visibility

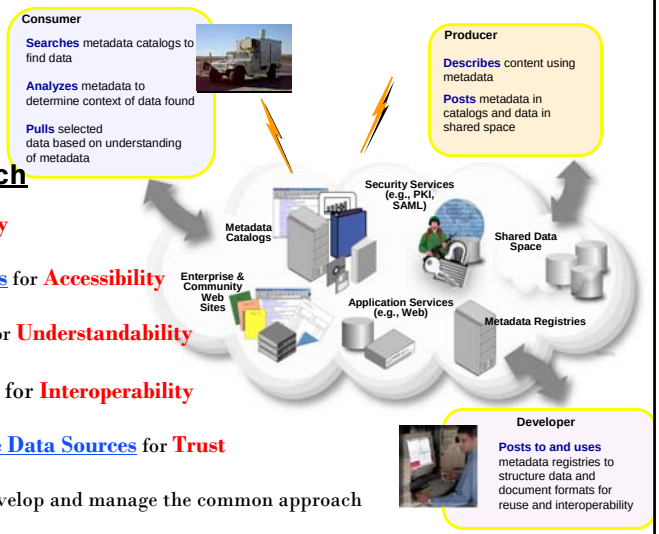
To Catalogs and Shared Spaces for Accessibility

Using Common Vocabulary for Understandability

Common Data Schema for Interoperability

Common Authoritative Data Sources for Trust

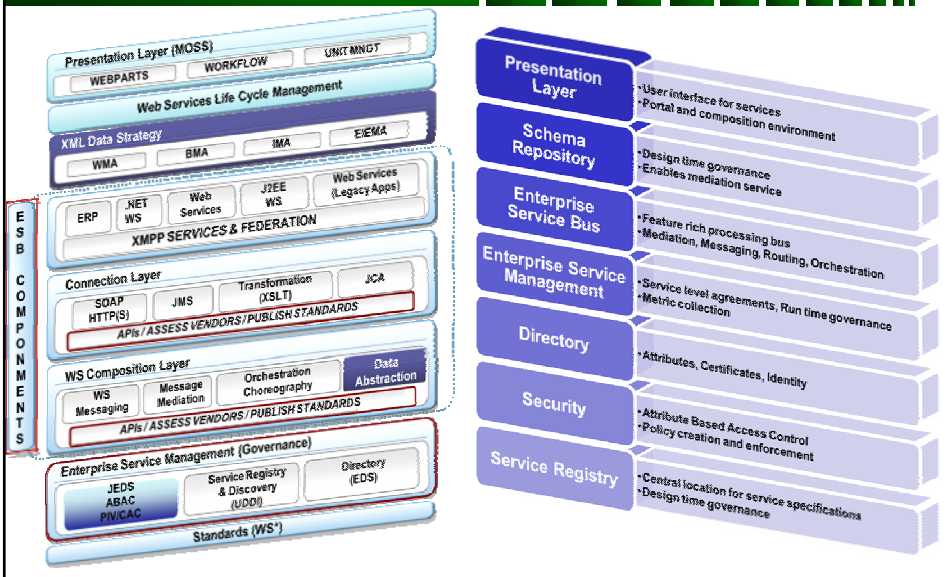
Communities of Interest to develop and manage the common approach



Paradigm Shift: From ownership to stewardship; From need-to-know to right-to-know; From stovepipes to enterprise; From programs to portfolios.

4

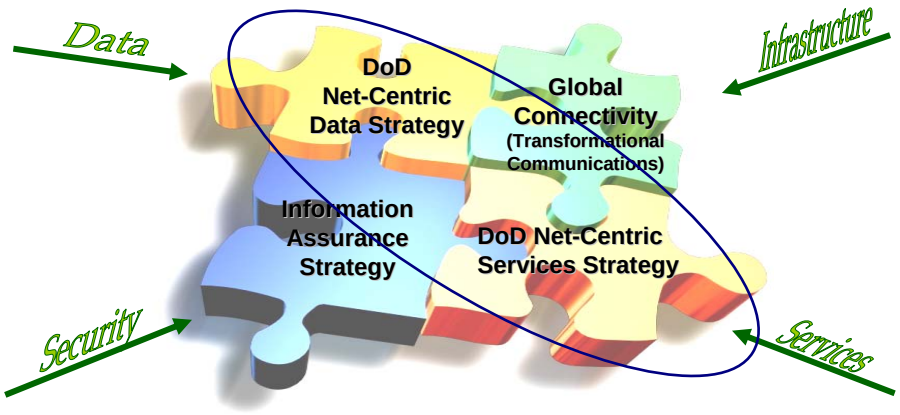
Army Enterprise SOA Foundation



5

Tenets of Net-Centric Operations

Global connectivity, real-time collaboration, and rapid and continuous information exchange



6

The Question

Okay, I get it. Data Strategy is important to achieving Net-Centricity. Service Oriented Architecture is important to achieving Net-Centricity. But how does SOA help me achieve the Data Strategy? How are they related?

Please explain in 30 words or less, Provide a PowerPoint Slide on the topic and an elevator speech so I can explain it to my General on his way to the to the next Net-Centric Discussion.*

*Graphic is for dramatization purposes only. The G3 staff officer wasn't actually holding weapon on us when he asked for the explanation. He was, however wearing sun glasses.

Data Strategy Goals and their meaning

Implementing the Strategy will enable data to be:

DoD Goals	Meaning
Visible	Who has what data available?
Accessible	Where is this data and in what format?
Institutionalized	What and who governs the definition, lifecycle, and use of this data?
Understandable	What does this data mean?
Trusted	Is this data trustworthy, accurate, and authoritative?
Interoperable	Can my application use this data?
Responsive	Is this data timely?

8

SOA Core Standards

DISCOVER (UDDI, XML Registries)	UDDI Registry is a conceptual phone book for Web Services. Organizations can register information about their Web Services and types of services with UDDI.
DESCRIBE (WSDL)	WSDL describes the operational information – where the service is located, what the service does, and how to talk to, or invoke the service.
ACCESS (SOAP)	SOAP is the envelope syntax for sending and receiving XML messages.
XML	XML is a text-based method and set of syntax rules for encoding (tagging) meta-data, allowing COIs to develop mission specific markup language. Does not provide semantic meaning and rules for information exchange.

SOA Core Standards provide the technical application and approach discussed in the Net-Centric Data Strategy supporting visibility, and accessibility, but ….. Semantic meaning and exchange rules are not addressed. The specification that captures the elements of the COI Ontology (Common understanding of Entities, Relationships, Properties, Values and Axioms/Rules) used by the XML markup language, UDDI Registries and COI defined Rules-based engines for information exchange is not addressed.

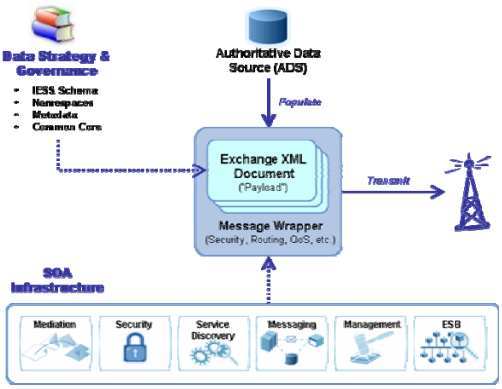
9

Supporting SOA Infrastructure Capabilities

- ***Service Discovery*** - provides the capabilities to publish and discover data, metadata, and services.
- ***Security*** - provides information assurance capabilities such as controlling access to services and data, management of user profiles and access control policies, message-level encryption and non-repudiation, etc.
- ***Reliable Messaging*** - provides the capability to reliably exchange messages between services and their consumers.
- ***Message and Protocol Mediation*** - provides the capability to adapt data formats and exchange protocols to enable interoperability in a heterogeneous environment.
- ***Service Orchestration*** - provides the capability to compose and orchestrate individual services into larger aggregates of functionality or business processes.
- ***Enterprise Service Management*** - provides the capabilities to monitor and control services to ensure compliance with defined contracts and service level agreements.

10

Data Strategy and SOA Roles in Net-Centric Data Exchange



The different focuses of a data strategy versus an SOA strategy make them in fact **complementary** – The data strategy by itself does not address the detailed messaging mechanisms for sending and receiving data across heterogeneous environments in a seamless and robust manner. This is precisely the purpose of the services environment that is created through an SOA strategy. On the other hand, the SOA strategy just provides a generic framework for exposing and sharing services—it says nothing about what should be shared through those services. This is where the data strategy comes in—it prescribes a strategy for identifying the data to be shared, where that data should be coming from (i.e. authoritative sources) and standard representations for sharing that data.

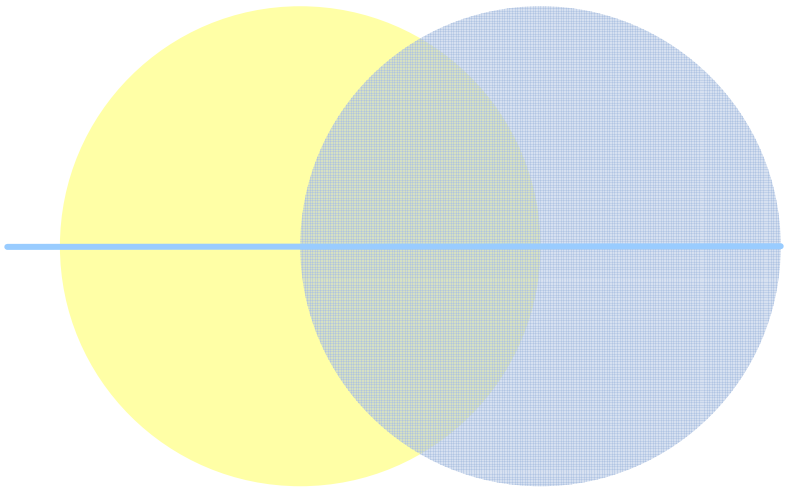
Service Oriented Architecture provides the **framework for orchestration** of data exchange.

Data Strategy provides the **governance approach, language and format** for data exchange.

The two strategies **intersect** in the areas of **Data Discovery and Retrieval** and **Data Mediation**.

11

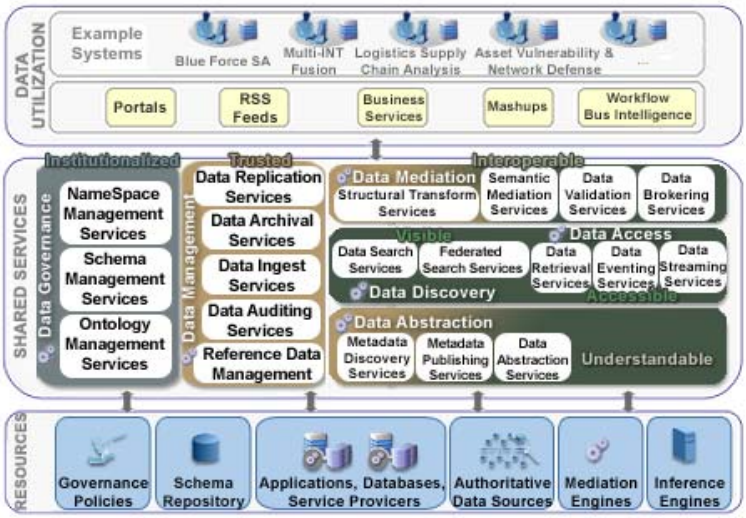
SOA – Data relationships and overlaps



The intersection of these two strategies results in the creation of an enterprise *data services layer* that enables sharing and management of data that is distributed across the enterprise.

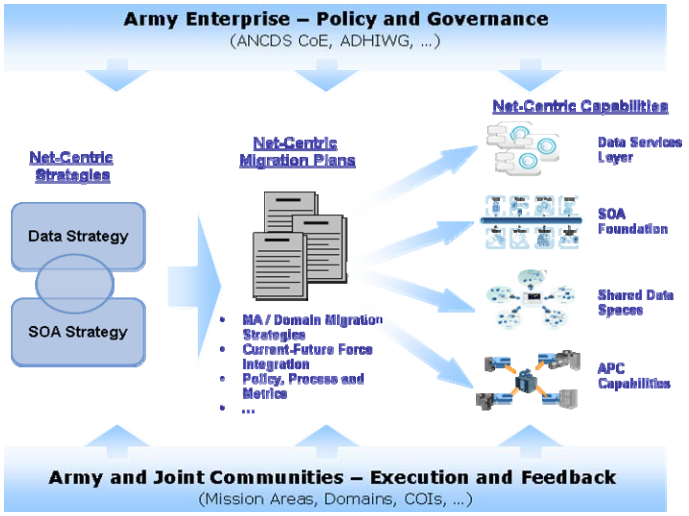
12

What is ADSL?



13

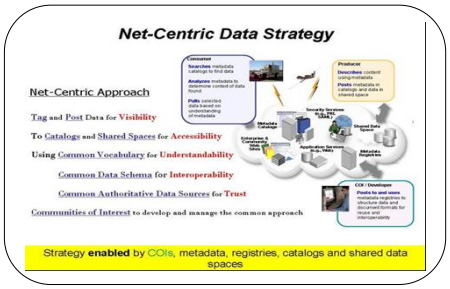
Data and SOA Strategies Driving Net-Centric Transformation

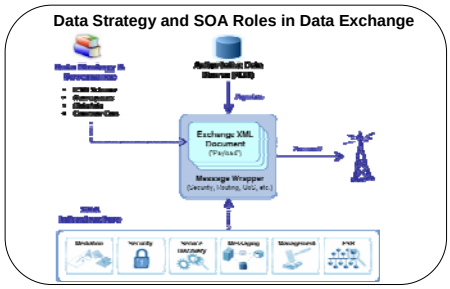


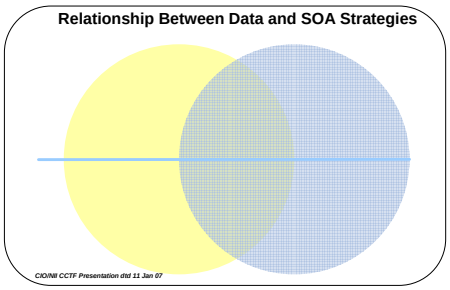
The close alignment of the Army Data and SOA strategies and the synergy between the two will help expedite the migration process towards building truly Net-Centric data capabilities, improve the effectiveness of enterprise governance, and increase community participation.

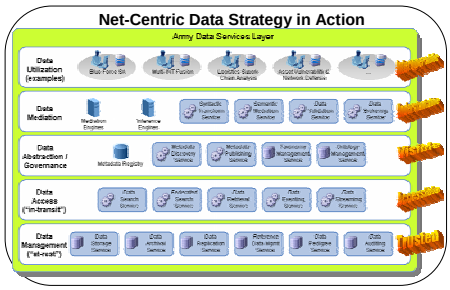
14

Data Strategy-SOA Relationship









15

Questions?

A
egy

- Service Portfolio Management
- Service Life Cycle
- Service Metrics

[SOA Foundation:]
- Security
- Service Discovery
- Messaging
- Orchestration
- …

16